UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/814,330	04/01/2004	Carl Rajsic	ALC 3124	5344

7590 08/31/2010

KRAMER & AMADO, P.C.
1725 Duke Street, Suite 240
Alexandria, VA 22314

EXAMINER	
MOORE JR, MICHAEL J	

ART UNIT	PAPER NUMBER
2467	

MAIL DATE	DELIVERY MODE
08/31/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte CARL RAJSIC

Appeal 2009-006982
Application 10/814,330
Technology Center 2400

Before KENNETH W. HAIRSTON, THOMAS S. HAHN, and BRADLEY W. BAUMEISTER, *Administrative Patent Judges.*

HAIRSTON, *Administrative Patent Judge.*

DECISION ON APPEAL[1]

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

Appellant seeks our review under 35 U.S.C. § 134(a) of the Examiner's final rejection of claims 1 to 13. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM-IN-PART.

Appellant's invention relates to multiservice switches (MSS) and a method for securely establishing Layer-3 switched virtual circuit (SVC) or soft permanent virtual circuit (SPVC) connections to carry internet protocol (IP) traffic over an asynchronous transfer mode (ATM) (Fig.1; Abstract; Spec. ¶¶ [01] and [02]). More specifically, Appellant discloses and claims configuring an MSS with security information to be sent in a setup message, analyzing the security information, and then establishing a Layer-3 connection depending on the outcome of the analysis (Abstract; Spec. ¶¶ [10], [14]-[17]; claims 1, 10 to 13). The MSSs provide customer premises equipment with access to the ATM network (Spec. ¶ [03]).

Claims 1 is representative of the claimed invention and reads as follows:

1. A method of establishing a secure Layer-3 connection across an ATM network, the Layer-3 connection having a first endpoint at an egress port of an originating multiservice switch (MSS) and a second endpoint at an ingress port of a terminating MSS, the method comprising the steps of:

configuring the terminating MSS with anticipated security information;

at the originating MSS, generating a setup message including embedded security information;

sending the setup message to the terminating MSS;

at the terminating MSS, extracting the embedded security information from the setup message;

determining whether the embedded security information matches the anticipated security information; and

if the embedded security information matches the anticipated security information, establishing the Layer-3 connection.

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Shirakawa	US 2002/0064159 A1	May 30, 2002
Bi	US 6,757,278 B1	Jun. 29, 2004 (filed Nov. 6, 2000)
Hall, Jr. (Hall)	US 7,130,393 B2	Oct. 31, 2006 (filed Jan. 20, 2000)

(i) The Examiner rejected claims 1, 4, 5, 7, and 9 to 13 under 35 U.S.C. § 102(e) as anticipated by Hall.

(ii) The Examiner rejected claims 2 and 3 under 35 U.S.C. § 103(a) based upon the teachings of Hall and Shirakawa.

(iii) The Examiner rejected claims 6 and 8 under 35 U.S.C. § 103(a) based upon the teachings of Hall and Bi.

With regard to the anticipation rejection of claims 1, 4, 5, 7, and 9 to 13, as well as the obviousness rejections of claims 2, 3, 6, and 8, the Examiner relies on Hall (*see* col. 8, ll. 2-9 and 21-24; col. 10, l. 23 to col. 11, l. 4; housing 10 and lens 28) as teaching the recited limitation of configuring an MSS with security information (Ans. 3-4 and 10-13). The Examiner finds that Hall's called party user group identifiers are equivalent to Appellant's recited "anticipated security information" (Ans. 10-11) and that

Hall teaches configuring an MSS with security information at column 19, lines 57-59 (Ans. 3, 12).

Appellant argues, *inter alia* (App. Br. 6-11; Reply Br. 4-5), that Hall (i) selects and operates on *all* closed user group identifiers instead of only the anticipated closed user group identifiers, (ii) fails to disclose the recited "anticipated security information," (iii) does not configure an MSS with anticipated security information but simply retrieves and makes the information readily available, and (iv) fails to disclose using closed user group interlock codes as recited in claim 4.

Based on Appellant's arguments, the issues presented are:

(i) Does the broadest reasonable interpretation of claims 1 and 10 to 13 encompass operating on *only* anticipated security information, as opposed to *all* security information?

(ii) Does Hall disclose "anticipated security information," as set forth in claims 1 and 10 to 13?

(iii) Does Hall disclose "configuring" an MSS with anticipated security information, as set forth in claim 1?

(iv) Does Hall disclose using closed user group interlock codes, as set forth in claim 4?

Because Appellant has not disputed the merits of the obviousness rejections of claims 2, 3, 6, and 8 other than to contend that (i) these claims are allowable for the same reasons as given for claim 1, (ii) these claims contain separately patentable subject matter that is not argued with particularity, and (iii) Shirakawa and Bi fail to cure argued deficiencies of Hall (*see* App. Br. 12), we will resolve the obviousness rejections of claims

2, 3, 6, and 8 for similar reasons provided *infra* with regard to the anticipation rejection of claim 1.

FINDINGS OF FACT (FF)

1. Appellant describes a method for securely establishing a Layer-3 connection using an ATM network 12 including originating multiservice switches (MSSs) (Spec. ¶¶ [01] and [02]). A setup message including security information is sent from an originating MSS 18 over an ATM network 12 to a terminating MSS 24 (Fig. 1). The security information may include a closed user group interlock code (Spec. ¶ [14). The terminating MSS 24 is configured with anticipated security information which can be a closed user group interlock code (Spec. ¶¶ [16], [17]; originally filed claim 1).
2. Hall describes an ATM network having closed user groups that authorizes calls using closed user group identifiers for a calling party and a receiving party (Abstract). Hall uses "various signaling or ATM messages" in the ATM network to setup and establish a switched virtual circuit connection between a calling party and a called party (col. 2, ll. 47-50), including an ATM setup message (col. 12, ll. 29-36; col. 14, ll. 10-17). Hall describes a method for establishing an SVC over an ATM network with closed user groups in the flowchart of Figure 5 (col. 18, l. 32 through col. 21, l. 37).
3. With regard to Figure 5, Hall states that ATM setup messages have certain information extracted from them and provided to the called party's switch (MSCP 44) "for analysis and closed user group service

processing" (col. 19, ll. 40-48; step 504 in Fig. 5). "All closed user group identifiers for the calling party, or calling user, are retrieved" (col. 19, ll. 48-50). Then, "all of the closed user group identifiers associated with the called party are retrieved or are made readily available" at step 506 (col. 19, ll. 57-59; step 506 in Fig. 5). In step 508 "a closed user group identifier that is common to both the calling party and the called party is found or located" (col. 20, ll. 1-3; step 508 in Fig. 5). At step 520, the call is authorized for the closed user group and a connection is established (col. 20, ll. 61-64; step 520 in Fig. 5).

4. With regard to the use of interlocking codes to authorize closed user group calls over an ATM network, Hall states that "the present invention provides advanced closed user group functionality, without the need or requirement of an interlocking code" (col. 19, ll. 34-36). Hall states that "the capability to provide interlock code functionality does not exist in ATM" (col. 3, ll. 46-48), and that interlock codes are not defined in ATM (col. 3, ll. 36-38).

PRINCIPLES OF LAW

Claim Construction

"During examination, 'claims … are to be given their broadest reasonable interpretation consistent with the specification, and … claim language should be read in light of the specification as it would be interpreted by one of ordinary skill in the art.'" *In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004); *In re Morris*, 127 F.3d 1048,

1053-54 (Fed. Cir. 1997). "[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (citation omitted).

Anticipation

Anticipation is established when a single prior art reference discloses, expressly or under the principles of inherency, each and every limitation of the claimed invention. *Atlas Powder Co. v. IRECO, Inc.*, 190 F.3d 1342, 1347 (Fed. Cir. 1999); *In re Paulsen*, 30 F.3d 1475, 1478-79 (Fed. Cir. 1994).

Obviousness

The Examiner's articulated reasoning for an obviousness rejection must possess a rational underpinning to support the legal conclusion of obviousness. *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006).

ANALYSIS

We agree with all of the Examiner's findings with regard to the anticipation rejection of claims 1, 5, 7, and 9 to 13, as well as the obviousness rejections of claims 2, 3, 6, and 8 (Ans. 3-12). With the exception of claim 4, we adopt the Examiner's findings of fact and conclusions of obviousness as our own. Because we agree with Appellant that Hall specifically teaches away from the use of interlock codes (*see* FF 4), we will not sustain the anticipation rejection of claim 4. We will sustain the Examiner's rejections of (i) claims 1, 5, 7, and 9 to 13 based upon the teachings of Hall; (ii) claims 2 and 3 based upon the teachings of Hall and

Shirakawa; and (iii) claims 6 and 8 based upon the teachings of Hall and Bi, for the reasons that follow.

Turning first to the anticipation rejection of claims 1, 5, 7, and 9 to 13, we are not persuaded by Appellant's arguments (App. Br. 7-10; Reply Br. 4-5) that Hall fails to select, compare, or operate on *only* anticipated security information, as opposed to *all* security information. Broadly interpreted, the recitations of claims 1, 5, 7, and 9 to 13 are met by Hall's operations on all of the closed user group identifiers (*see* FF 3). *Am. Acad. of Sci. Tech Ctr.*, 367 F.3d at 1364.

The phrase "only" does not occur in claims 1, 5, 7, and 9 to 13, nor do these claims limit operations to just a subset or part of the security information. In our view, independent claims 1, and 10 to 13 do not encompass the concept of operating on *only* part of the security information. Inasmuch as Appellant's arguments in this regard are not commensurate with the language of the claims, this line of reasoning is not persuasive.

We find that Hall discloses anticipated security information and embedded security information inasmuch as Hall's security information (i.e., closed user group identifiers for called parties and calling parties) performs the same function as Appellant's security information used for call setup and authorization for a Layer-3 connection in a closed user group over an ATM network (*compare* FF 1 *with* FF 2 and 3). The security information recited in claim 1 would be reasonably understood by one of ordinary skill in the art to encompass Hall's closed user group identifiers for called and calling parties because a call is authorized and established based on a check of the closed user group identifiers (FF 2 and 3).

With regard to the "configuring . . . " limitation of claim 1, we find that Appellant's originally filed Specification and claims (*see* FF1) do not define the phrase "configuring" or otherwise describe this term. We find that Hall discloses using setup messages for closed user groups in ATM networks, and that the setup messages include closed user group identifiers for called parties that "are retrieved or *made readily available*" (FF 3 (emphasis added)). Therefore, we determine that Hall discloses "configuring" an MSS (MSCP 44) with anticipated security information as set forth in original claim 1 and as defined by paragraphs [16] and [17] of the Specification.

Thus, we find no error in the Examiner's reliance on Hall as teaching the configuring limitation, at least to the extent this feature is broadly recited in claim 1 and defined in the Specification. *See Am. Acad. of Sci. Tech Ctr.*, 367 F.3d at 1364; *Phillips*, 415 F.3d at 1315. Appellant has not shown that the Examiner erred in determining that Hall discloses an MSS with configuring anticipated security information, as set forth in claim 1 and claims 5, 7, and 9 that depend therefrom.

With regard to claim 4, Appellant's argument (App. Br. 10-11) that Hall fails to disclose using closed user group *interlock codes* as recited in claim 4 is convincing. While Hall describes the use of interlocking codes to authorize closed user group calls over an ATM network, Hall's disclosed invention does so "without the need or requirement of an interlocking code" (col. 19, ll. 34-36; FF 4). Hall teaches away from the use of interlock codes in ATM networks (see FF 4), and instead uses *identifiers* to provide closed user group functionality in an ATM network (FF 3 and 4). Because Hall

fails to disclose each and every limitation of the claimed invention, we will not sustain the anticipation rejection of claim 4. *Atlas Powder Co.*, 190 F.3d at 1347; *Paulsen*, 30 F.3d at 1478-79.

Turning next to the obviousness rejections of claims 2, 3, 6, and 8, Appellant does not separately argue with particularity the limitations of these claims apart from merely asserting that these claims recite further features that are not taught or suggested by cited prior art (App. Br. 12). Such conclusory assertions without supporting explanation or analysis particularly pointing out errors in the Examiner's reasoning fall well short of persuasively rebutting the Examiner's prima facie case of obviousness. *See In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992). Accordingly, we will sustain the obviousness rejections of claims 2, 3, 6, and 8 for similar reasons provided *supra* with regard to the anticipation rejection of claim 1.

CONCLUSIONS

Hall explicitly or inherently discloses multiservice switches and a method, and computer program performing a method, for establishing a secure Layer-3 connection across an ATM network, as set forth in claims 1 and 10 to 13. Hall discloses "anticipated security information" (independent claims 1 and 10 to 13) and "configuring" (claim 1) or embedding an MSS with such information (claims 10 to 13).

Hall does not teach the interlock codes set forth in claim 4.

Appellant has not shown the Examiner erred in rejecting claims 1, 5, 7, and 9 to 13 under 35 U.S.C. § 102(e) or claims 2, 3, 6, and 8 under 35

U.S.C. § 103(a). Appellant has shown the Examiner erred in rejecting claim 4 under 35 U.S.C. § 102(e).

ORDER

The decision of the Examiner rejecting claims 1 to 3 and 5 to 13 is affirmed. The decision of the Examiner rejecting claim 4 is reversed. Accordingly, the decision of the Examiner is affirmed-in-part.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(v).

AFFIRMED-IN-PART

ELD

KRAMER & AMADO, P.C.
1725 DUKE STREET, SUITE 240
ALEXANDRIA, VA 22314